

# EXHIBIT

# 42

268

UNITED STATES ATTORNEY GENERAL  
CRIMINAL DIVISION

Department of Justice  
Washington, D.C. 20530

11-1-78  
11-1-78

MEMORANDUM TO DR. FRANK PRESS  
Science Advisor to the President

Re: Constitutionality Under the First Amendment  
of ITAR Restrictions on Public Cryptography

The purpose of this memorandum is to discuss the constitutionality under the First Amendment of restrictions imposed by the International Traffic in Arms Regulation (ITAR), 22 C.F.R. § 121 et seq. (1977), the regulation implementing § 38 of the Arms Export Control Act, 22 U.S.C.A. § 2778 (1977), on dissemination of cryptographic information developed independent of government supervision or support by scientists and mathematicians in the private sector.<sup>1/</sup> Our discussion is confined to the applicability of the regulation to the speech elements of public cryptography, and does not address the validity of the general regulatory controls over exports of arms and related items. We have undertaken our review of the First Amendment issues raised by the ITAR as an outgrowth of our role in implementing Presidential Directive NSC-24.<sup>2/</sup>

<sup>1/</sup> The cryptographic research and development of scientists and mathematicians in the private sector is known as "public cryptography." As you know, the serious concern expressed by the academic community over government controls of public cryptography, see, e.g., 197 Science 1345 (Sept. 30, 1977), led the Senate Select Committee on Intelligence to conduct a recently concluded study of certain aspects of the field.

<sup>2/</sup> Our research into the First Amendment issues raised by government regulation of public cryptography led tangentially into broader issues of governmental control over dissemination of technical data. Those questions are numerous, complex, and deserving of extensive study, but are beyond the scope of this memorandum.

participation in briefings and symposia) and disclosed to foreign nationals in the United States (including plant visits and participation in briefings and symposia).

Thus ITAR requires licensing of any communication of cryptographic information,<sup>4/</sup> whether developed by the government or by private researchers, which reaches a foreign national.<sup>5/</sup>

The standards governing license denial are set out in § 123.05. The Department of State may deny, revoke, suspend or amend a license:

whenever the Department deems such action to be advisable in furtherance of (1) world peace; (2) the security of the United States; (3) the foreign policy of the United States; or (4) whenever the Department has reason to believe that section 414 of the Mutual Security Act of 1954, as amended, or any regulation contained in this subchapter shall have been violated.

Upon any adverse decision, the applicant may present additional information and obtain a review of the case by the

<sup>4/</sup> The ITAR does exempt from the licensing requirement unclassified technical data available in published form. 22 C.F.R. § 125.11(a). The scope of that exemption is somewhat unclear, although it does appear that the burden of ascertaining the ITAR status of possibly exempt information is on the individual seeking publication. See 22 C.F.R. § 125 n.3. In order to claim the exemption, an "exporter" must comply with certain certification procedures. 22 C.F.R. § 125.22.

<sup>5/</sup> For example, in one instance the Office of Munitions Control, the office in the State Department which administers the ITAR, refused to issue licenses to a group of scientists preparing to address a conference on space technology in Madrid. The scientists, who had already arrived in Spain, were refused permission to deliver papers at the symposium on the subject of rocket propulsion and re-entry problems of space vehicles. Note, Arms Control-State Department Regulation of Exports of Technical Data Relating to Munitions Held to Encompass General Knowledge and Experience, 9 N.Y.U. Int'l Law J. 91, 101 (1976).

ITAR Provisions and Statutory Authority

Under the ITAR, exports of articles designated on the United States Munitions List as "arms, ammunition, and implements of war" must be licensed by the Department of State. 22 C.F.R. §§ 123, 125. Cryptographic devices are included on the list, 22 C.F.R. § 121.01, Category XIII, as are related classified and unclassified technical data, Category XVII, Category XVIII. It is this control over the export of unclassified technical data which raises the principal constitutional questions under the ITAR.<sup>3/</sup>

The broad definition of the term technical data in the ITAR includes:

Any unclassified information that can be used, or be adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance, or reconstruction of arms, ammunition and implements of war on the U.S. Munitions List.

22 C.F.R. § 125.01. The definition of the term "export" is equally broad. Under § 125.03 of the ITAR an export of technical data takes place:

Whenever technical data is inter alia, mailed or shipped outside the United States, carried by hand outside the United States, disclosed through visits abroad by American citizens (including

<sup>3/</sup> Unclassified technical data would generally encompass only privately developed, nongovernmental cryptographic research. It is our understanding that government-sponsored cryptographic research traditionally has been classified. The only unclassified government cryptographic information of which we are aware is the Data Encryption Standard (DES) algorithm. The DES was developed for public use by IBM with National Security Agency assistance and published in the Federal Register by the National Bureau of Standards.



Department. § 123.05(c). No further review is provided.

Nearly all of the present provisions of the ITAR were originally promulgated under § 414 of the Mutual Security Act of 1954 (former 22 U.S.C. § 1934). That statute gave the President broad authority to identify and control the export of arms, ammunition, and implements of war, including related technical data, in the interest of the security and foreign policy of the United States. Congress recently substituted for that statute a new § 38 of the Arms Export Control Act, 22 U.S.C.A. § 2778 (1977), as amended, 22 U.S.C.A. § 2778 (Supp. 3 1977). This statute substitutes the term "defense articles and defense services" for the term "arms, ammunition, and implements of war."<sup>6/</sup> The President delegated his authority under both statutes to the Secretary of State and Secretary of Defense. Exec. Order No. 11,958, 42 Fed. Reg. 4311 (1977), reprinted in 22 U.S.C.A. § 2778 (Supp. 1 1977); Exec. Order No. 10,973, 3 C.F.R. 493 (Supp. 1964). A willful violation of § 38 of the Arms Export Control Act or any regulation thereunder is punishable by a fine up to \$100,000, imprisonment up to two years, or both. 22 U.S.C.A. § 2778(c).<sup>7/</sup>

<sup>6/</sup> The ITAR has not yet been amended to reflect the statutory change. We understand, however, that the Department of State has nearly completed a draft revision of the ITAR. It is our understanding that the revision is not intended to make any major substantive changes in the ITAR, but rather to update and clarify the regulatory language.

<sup>7/</sup> Although the focus of this memorandum is on the First Amendment issues raised by the ITAR, we feel that one comment about the breadth of the two statutes is in order. It is by no means clear from the language or legislative history of either statute that Congress intended that the President regulate noncommercial dissemination of information, or considered the problems such regulation would engender. We therefore have some doubt whether § 38 of the Arms Export Control Act provides adequate authorization for the broad controls over public cryptography which the ITAR imposes.

The First Amendment Issues

The ITAR requirement of a license as a prerequisite to "exports" of cryptographic information clearly raises First Amendment questions of prior restraint.<sup>8/</sup> As far as we have been able to determine, the First Amendment implications of the ITAR have received scant judicial attention.

The Ninth Circuit presently has a case under consideration which squarely presents a First Amendment challenge to the ITAR and could serve as a vehicle for the first comprehensive judicial analysis of its constitutionality. In that case, United States v. Edler, No. 76-3370, the defendants, Edler Industries, Inc. and Vernon Edler its president, were charged with exporting without a license technical data and assistance relating to the fabrication of missile components. Although the State Department had denied defendants an export license to provide technical data and assistance to a French aerospace firm, the government alleged that defendants nonetheless delivered data and information to the French during meetings in both France and the United States. Defendants were tried before a jury and found guilty. The trial court, the United States District Court for the Central District of California, did not issue an opinion in the case. On appeal, the defendants contend that the ITAR is both overbroad and establishes an unconstitutional prior restraint. The government's rejoinder to those claims is that the ITAR licensing provisions involve conduct not speech and that any effect upon First Amendment freedoms is merely incidental.

<sup>8/</sup> In addition, the regulatory provisions present questions of overbreadth and vagueness. "Overbreadth" is a First Amendment doctrine invalidating statutes which encompass, in a substantial number of their applications, both protected and unprotected activity. The "vagueness" concept, on the other hand, originally derives from the due process guarantee, and applies where language of a statute is insufficiently clear to provide notice of the activity prohibited. The same statute or regulation may raise overlapping questions under both doctrines.

and therefore valid. We anticipate that the resolution of these issues by the Ninth Circuit may provide substantial guidance as to the First Amendment implications of the ITAR.<sup>9/</sup>

The only published decision addressing a First Amendment challenge to the ITAR of which we are aware is United States v. Donas-Botto, 363 F.Supp. 191 (E.D. Mich. 1973), aff'd sub nom. United States v. Van Hee, 531 F.2d 352 (6th Cir. 1976). The defendants in that case were charged with conspiracy to export technical data concerning a Munitions List item without first obtaining an export license or written State Department approval. The exports by the defendants both of blueprints and of their technical knowledge concerning an armored amphibious vehicle were alleged to be in violation of § 414 of the Mutual Security Act and the ITAR. In a motion to dismiss the indictments, defendants contended that inclusion of technical knowledge within the statute violated the First Amendment. The trial court disposed of that contention summarily, stating:

[W]hen matters of foreign policy are involved the government has the constitutional authority to prohibit individuals from divulging "technical data" related to implements of war to foreign governments.

363 F. Supp. at 194. The Sixth Circuit upheld the conviction of one of the defendants without reaching any First Amendment questions since none was presented on appeal.<sup>10/</sup>

The First Amendment analysis of the ITAR in the case thus is limited to a paragraph in the district court's opinion. In reaching the conclusion that the prosecutions did not violate the First Amendment, that court relied upon two Espionage Act decisions, Gorin v. United States, 312 U.S.

<sup>9/</sup> We understand that the case was argued this past March.

<sup>10/</sup> The court did agree with the trial judge that the ample scope of the term "technical data" in the ITAR encompassed unwritten technical knowledge. 531 F.2d at 537.



19 (1941), and United States v. Rosenberg, 195 F.2d 583 (2d Cir.), cert. denied, 344 U.S. 838 (1952). While those cases establish that the First Amendment does not bar prosecutions for disclosing national defense information to a foreign country, they by no means resolve the prior restraint question.<sup>11/</sup>

A decision in a somewhat analogous area, the use of secrecy agreements by government agencies as a means of protecting against the unauthorized disclosure of information by present or former employees, while not directly applicable to the First Amendment questions we confront under the ITAR, is helpful for its discussion of government's power to control the dissemination of government information. That case, United States v. Marchetti, 466 F.2d 1309 (4th Cir.), cert. denied, 409 U.S. 1063 (1972), after remand, Alfred A. Knopf, Inc. v. Colby, 509 F.2d 1362 (4th Cir.), cert. denied, 421 U.S. 992 (1975), involved an action for an injunction brought by the United States to prevent a former CIA agent from publishing certain information he had obtained as a result of his CIA employment. The court held that the particular secrecy agreement was valid and enforceable in spite of Marchetti's First Amendment objections, but observed that:

The First Amendment limits the extent to which the United States, contractually or otherwise, may impose secrecy agreements upon its employees and enforce them with a system of prior censorship. It precludes such restraints with respect to information which is unclassified or officially disclosed.

Id. at 1313. The general principle we derive from the case is that a prior restraint on disclosure of information generated by or obtained from the government is justifiable under the First Amendment only to the extent that the information is properly classified or classifiable.

<sup>11/</sup> It is not clear from reading the district court's opinion on what First Amendment ground or grounds the defendants based their unsuccessful motion to dismiss.



Our research into areas in which the government has restricted disclosure of nongovernmental information provided little additional guidance. Perhaps the closest analogy to controls over public cryptography are the controls over atomic energy research.<sup>12/</sup> Under the Atomic Energy Act of 1954, 42 U.S.C. § 2011 et seq. (1970), all atomic energy information, whether developed by the government or by private researchers, is automatically classified at its creation and subjected to strict nondisclosure controls.<sup>13/</sup> Although neither the Atomic Energy Act nor its accompanying regulations establish formal procedures for prior review of proposed atomic energy publications, the Atomic Energy Commission (whose functions are now divided

<sup>12/</sup> Atomic energy research is similar in a number of ways to cryptographic research. Development in both fields has been dominated by government. The results of government created or sponsored research in both fields have been automatically classified because of the imminent danger to national security flowing from disclosure. Yet meaningful research in the fields may be done without access to government information. The results of both atomic energy and cryptographic research have significant nongovernmental uses in addition to military use. The principal difference between the fields is that many atomic energy researchers must depend upon the government to obtain the radioactive source materials necessary in their research. Cryptographers, however, need only obtain access to an adequate computer.

<sup>13/</sup> See Green, Information Control and Atomic Power Development, 21 Law and Contemporary Problems 91 (1956); Newman, Control of Information Related to Atomic Energy, 56 Yale L.J. 769 (1947). The Atomic Energy Act uses the term "Restricted Data" to describe information which the government believes requires protection in the interest of national security. "Restricted data" is defined in 42 U.S.C. § 2014(4). The information control provisions of the Act are set out at 42 U.S.C. §§ 2161-2164.

between the Nuclear Regulatory Commission and the Department of Energy) has been empowered to maintain control over publications through threat of injunction or of heavy criminal penalties, two potent enforcement tools provided under the Act. 42 U.S.C. §§ 2271-2277, 2280. It does not seem, however, that the broad information controls of the Atomic Energy Act have ever been challenged on First Amendment grounds. Our search for judicial decisions in other areas in which the government has imposed controls over the flow of privately generated information was equally unavailing.<sup>14/</sup>

In assessing the constitutionality of the ITAR restrictions on the speech elements of public cryptography we therefore have turned to Supreme Court decisions enunciating general First Amendment principles. It is well established that prior restraints on publication are permissible only in extremely narrow circumstances and that the burden on the government of sustaining any such restraint is a heavy one. See, e.g., Nebraska Press Association v. Stuart, 427 U.S. 539 (1976); New York Times Co. v. United States, 403 U.S. 713 (1971); Organization for a Better Austin v. Keefe, 402 U.S. 415 (1971); Carroll v. Princess Anne, 393 U.S. 175 (1968); Near v. Minnesota, 283 U.S. 697 (1931). Even in those limited circumstances in which prior restraints have been deemed constitutionally permissible, they have been circumscribed by specific, narrowly drawn standards for deciding whether to prohibit disclosure and by substantial procedural protections. Erznoznik v. City of Jacksonville, 422 U.S. 205 (1975); Blount v. Rizzi, 400 U.S. 410 (1971); Freedman v. Maryland, 380 U.S. 51 (1965); Niemotko v. Maryland,

<sup>14/</sup> For example, it does not appear that the broad controls over exports of technical data and related information under the Export Administration Act of 1969, 50 U.S.C. App. § 2401 et seq. (1970), and accompanying regulations have been judicially tested on First Amendment grounds. Nor have the provisions of the patent laws restricting patentability of inventions affecting national security, 35 U.S.C. § 181 et seq. (1970), nor governmental restrictions on communications with Rhodesia, 22 U.S.C. § 287c (1970); Exec. Order No. 11,322

340 U.S. 268 (1951); Kunz v. New York, 340 U.S. 290 (1951)  
Hague v. C.I.O., 307 U.S. 496 (1939).<sup>15/</sup>

Even if it is assumed that the government's interest in regulating the flow of cryptographic information is sufficient to justify some form of prior review process, the existing ITAR provisions we think fall short of satisfying the strictures necessary to survive close scrutiny under the First Amendment. There are at least two fundamental flaws in the regulation as it is now drawn: first, the standards governing the issuance or denial of licenses are not sufficiently precise to guard against arbitrary and inconsistent administrative action; second, there is no mechanism established to provide prompt judicial review of State Department decisions barring disclosure. See, e.g., Blount v. Rizzi, supra; Freedman v. Maryland, supra; Hague v. C.I.O., supra. The cases make clear that before any restraint upon protected expression may become final it must be subjected to prompt judicial review in a proceeding in which the government will bear the burden of justifying its decisions. The burden of bringing a judicial proceeding cannot be imposed upon those desiring export licenses in these circumstances. The ITAR as presently written fails to contemplate this requirement.<sup>16/</sup>

<sup>15/</sup> In Freedman, 380 U.S. at 58-59, the Court summarized the procedural protections necessary to sustain a scheme of prior review:

1. A valid final restraint may be imposed only upon a judicial determination;
2. The administrator of a licensing scheme must act within a specified brief period of time;
3. The administrator must be required either to issue a license or go to court to seek a restraint;
4. Any restraint imposed in advance of a final judicial determination on the merits must be limited to preservation of the status quo for the shortest period compatible with sound judicial resolution;
5. The licensing scheme must assure a prompt final judicial decision reviewing any interim and possibly erroneous denial of a license.

<sup>16/</sup> The government's argument to the Ninth Circuit in Edler, that the impact of the ITAR upon protected communications is merely incidental, and that the ITAR should be viewed as  
 (Cont. on p. 11)



For these reasons it is our conclusion that the present ITAR licensing scheme does not meet constitutional standards. There remains the more difficult question whether a licensing scheme covering either exports of or even purely domestic publications of cryptographic information might be devised consistent with the First Amendment. Recent Supreme Court decisions certainly suggest that the showing necessary to sustain a prior restraint on protected expression is an onerous one. The Court held in the Pentagon Papers case that the government's allegations of grave danger to the national security provided an insufficient foundation for enjoining disclosure by the Washington Post and the New York Times of classified documents concerning United States activities in Vietnam. New York Times Co. v. United States, supra.<sup>17/</sup> The Court also invalidated prior restraints when justified by such strong interests as the right to fair trial, Nebraska Press Ass'n, supra, and the right of a homeowner to privacy, Organization for a Better Austin v. Keefe, supra. Such decisions raise a question whether a

<sup>16/</sup> (Cont.)

a regulation of conduct not speech, deserves note. According to that argument, the less rigorous constitutional standard of United States v. O'Brien, 391 U.S. 367 (1968), would govern the validity of the ITAR. Although that may be true with respect to certain portions of the ITAR, even a cursory reading of the technical data provisions reveals that those portions of the ITAR are directed at communication. A more stringent constitutional analysis than the O'Brien test is therefore mandated.

<sup>17/</sup> The Pentagon Papers case produced a total of ten opinions from the Court, a per curiam and nine separate opinions. All but Justices Black and Douglas appeared willing to accept prior restraints on the basis of danger to the national security in some circumstances. There was, however, no agreement among the Justices on the appropriate standard. Justice Brennan stated his view that a prior restraint on publication was justified only upon:

"proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea. . . ."

(Cont. on p. 12)



generalized claim of threat to national security from publication of cryptographic information would constitute an adequate basis for establishing a prior restraint. Nonetheless, it is important to keep in mind that the Court has consistently rejected the proposition that prior restraints can never be employed. See, e.g., Nebraska Press Ass'n, *supra* at 570. For example, at least where properly classified government information is involved, a prior review requirement may be permissible. United States v. Marchetti, *supra*.

In evaluating the conflicting First Amendment and national security interests presented by prior restraints on public cryptography, we have focused on the basic values which the First Amendment guarantees. At the core of the First Amendment is the right of individuals freely to express political opinions and beliefs and to criticize the operations of government. See, e.g., Landmark Communications v. Virginia, 46 U.S.L.W. 4389, 4392 (May 1, 1978); Buckley v. Valeo, 424 U.S. 1, 14 (1976); Mills v. Alabama, 384 U.S. 214, 218 (1966). Adoption of the Amendment reflected a "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open," New York Times v. Sullivan, 376 U.S. 254, 270 (1964), and was intended in part to prevent use of seditious libel laws to stifle discussion of information embarrassing to the government. New York Times Co. v. United States, *supra* at 724 (concurring opinion of Mr. Justice Douglas).

Prior restraints pose special and very serious threats to open discussion of questions of public interest. "If it can be said that a threat of criminal or civil sanctions after publication 'chills' speech, prior restraint 'freezes' it at least for the time." Nebraska Press Ass'n, *supra* at 559.

17/ (Cont.)

403 U.S. at 726-27. Justice Stewart, with whom Justice White concurred, suggested that a prior restraint would be permissible only if disclosure would "surely result in direct, immediate and irreparable damage to our Nation or its people." *Id.* at 730. Several other Justices declined, given the facts and procedural posture of the case, to formulate a standard.

Since views on governmental operations or decisions often must be aired promptly to have any real effect, even a temporary delay in communication may have the effect of severely diluting "uninhibited, robust, and wide-open" debate. And protection of any governmental interest may usually be accomplished by less restrictive means. One avenue generally available to the government, and cited by Supreme Court as the most appropriate antedote, is to counter public disclosures or criticisms with publication of its own views. See, e.g., Whitney v. California, 274 U.S. 357, 375 (1927) (concurring opinion of Mr. Justice Brandeis).

The effect of a prior restraint on cryptographic information, however, differs significantly from classic restraints on political speech. Cryptography is a highly specialized field with an audience limited to a fairly select group of scientists and mathematicians. The concepts and techniques which public cryptographers seek to express in connection with their research would not appear to have the same topical content as ideas about political, economic or social issues. A temporary delay in communicating the results of or ideas about cryptographic research therefore would probably not deprive the subsequent publication of its full impact.

Cryptographic information is, moreover, a category of matter "which is both vital and vulnerable to an almost unique degree."<sup>18/</sup> Once cryptographic information is disclosed, the damage to the government's interest in protecting

<sup>18/</sup> New York Times Co. v. United States, 403 U.S. 713, 736 n. 7 quoting H.R. Rep. No. 1895, 81st Cong., 2d Sess., 1 (1950). That report pertains to the bill which became 18 U.S.C. § 798, the criminal statute prohibiting disclosure of information concerning the cryptographic systems and communications intelligence activities of the United States. Section 798 does not reach disclosure of information published by public cryptographers, as its coverage is restricted to classified information. Classified information by definition is information in which the government has some proprietary interest. See § 1(b) of the May 3, 1978 draft of the Executive Order on national security proposed to replace Executive Order 11,652; cf. 22 C.F.R. § 125.02.

national security is done and may not be cured. Publication of cryptographic information thus may present the rare situation in which "more speech" is not an alternative remedy to silence.<sup>19/</sup> See Whitney v. California, supra at 376 (concurring opinion of Mr. Justice Brandeis).

Given the highly specialized nature of cryptographic information and its potential for seriously and irretrievably impairing the national security, it is our opinion that a licensing scheme requiring prepublication submission of cryptographic information might overcome the strong constitutional presumption against prior restraints. Any such scheme must, as we have said, provide clear, narrowly defined standards and procedural safeguards to prevent abuse.

While a detailed discussion of the specific provisions and procedures of a valid scheme of prior review of cryptographic information or of its practical and political feasibility is beyond the scope of this memorandum, some

<sup>19/</sup> In stressing the differences between cryptographic information and other forms of expression we do not mean to imply that the protections of the First Amendment are not applicable to cryptographic information or that they are confined to the exposition of ideas. See Winters v. New York, 333 U.S. 507, 510 (1948). We recognize that the scope of the amendment is broad. It encompasses, for example, purely commercial speech, Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc. 425 U.S. 748 (1976), and communicative conduct, Cohen v. California 403 U.S. 15 (1971). We believe, however, that the extent of First Amendment protection may vary depending upon the nature of communication at issue. It is established in the area of commercial speech that greater governmental regulation may be tolerated due to the special attributes of that form of speech. Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, supra at 770-71 and n.24. Speech in the labor context also presents special First Amendment considerations. See, e.g., N.L.R.B. v. Gissel Packing Co., 395 U.S. 575 (1969). And obscene communications have received specialized treatment from the courts. See, e.g., Roth v. United States, 354 U.S. 476 (1957).



general observations are in order. First, we wish to emphasize our doubts that the executive branch may validly provide for licensing or prior review of exports of cryptographic information without more explicit Congressional authorization. The scope of the existing delegation of authority from Congress to the President, as we note above, is somewhat unclear. Before imposing a prior restraint on exports of public cryptographic information, we believe that a more clear cut indication of Congressional judgment concerning the need for such a measure is in order. See United States v. Robel, 389 U.S. 248, 269 (1967) (concurring opinion of Mr. Justice Brennan); cf. Yakus v. United States, 321 U.S. 414 (1944). Some of this  
note 7.

Second, further Congressional authorization would obviously be necessary in order to extend governmental controls to domestic as well as foreign disclosures of public cryptographic information. Such an extension might well be necessary to protect valuable cryptographic information effectively. Indeed, limiting controls to exports while permitting unregulated domestic publication of cryptographic research would appear to undermine substantially the government's position that disclosure of cryptographic information presents a serious and irremediable threat to national security.<sup>20/</sup>

<sup>20/</sup> A question which would arise from complete governmental control over cryptographic information is whether the government would be required under the Fifth Amendment to pay just compensation for the ideas it had effectively "condemned." For example, the patent and invention provisions of the Atomic Energy Act require the government to pay for patents which it revokes or declares to be affected with the public interest. 42 U.S.C. §§ 2181-2190. A cryptographic algorithm, however, would not appear to be a patentable process. See Gottschalk v. Benson, 409 U.S. 63 (1972). And it is unresolved whether copyright protection is available for computer software. See Nimmer on Copyright, § 13.1 (Supp. 1976). We are therefore uncertain as to the status of cryptographic ideas under the Fifth Amendment.



Third, no final restraint on disclosure may be imposed without a judicial determination. We recognize that a requirement of judicial review presents substantial problems. The proof necessary in order to demonstrate to a judge that highly technical cryptographic information must be withheld from publication because of the overriding danger to national security might be burdensome and might itself endanger the secrecy of that information. It is our opinion, however, that any system which failed to impose the burden on government of seeking judicial review would not be constitutional.<sup>21/</sup> See, e.g., Blount v. Rizzi, *supra*.

Finally, any scheme for prior review of cryptographic information should define as narrowly and precisely as possible both the class of information which the government must review to identify serious threats to the national security and the class of information which the government must withhold.<sup>22/</sup> The scheme clearly should exempt from a

<sup>21/</sup> The threat to national security posed by a judicial review procedure could be reduced substantially by conducting the review in camera. See Alfred A. Knopf, Inc. v. Colby, 509 F.2d 1362 (4th Cir.), *cert. denied*, 421 U.S. 992 (1975); *cf.* 5 U.S.C. 552(a)(4)(B) (Supp. 1975) (in camera review provision of the Freedom of Information Act). The Supreme Court, in any event, has been unimpressed by arguments that disclosure of sensitive national security information to a court raises such serious problems of public dissemination that exemption from constitutional requirements is appropriate. See United States v. U.S. District Court, 407 U.S. 297 (1972).

<sup>22/</sup> In other words, we assume that the information submitted under the scheme would not be coextensive with the information withheld. We note, however, that the authority of the government to require prepublication submission of information which is neither classified nor classifiable is unsettled. That issue is posed in the suit recently filed by the Department of Justice in the United States District Court for the Eastern District of Virginia against former CIA employee Frank Snepp for breach of his secrecy agreement. United States v. Snepp, Civil Action No. 78-92-A.

submission requirement any information, such as that which is publicly available or which poses no substantial security threat, that the government has no legitimate interest in keeping secret.<sup>23/</sup> Failure to draft provisions narrowly might well invite overbreadth challenges for inclusion of protected communication. See, e.g., NAACP v. Alabama, 357 U.S. 449 (1958). And a precisely drawn scheme is also necessary to avoid objections of vagueness. See, e.g., Smith v. Goguen, 415 U.S. 566 (1974).<sup>24/</sup>

In conclusion, it is our view that the existing provisions of the ITAR are unconstitutional insofar as they establish a prior restraint on disclosure of cryptographic ideas and information developed by scientists and mathematicians in the private sector. We believe, however, that a prepublication review requirement for cryptographic information might meet First Amendment standards if it provided necessary procedural safeguards and precisely drawn guidelines.



John M. Harmon  
Assistant Attorney General  
Office of Legal Counsel

<sup>23/</sup> As we noted above, at n.4, supra, the present ITAR provisions attempt to exempt publicly available information. But the scope of that exemption and the procedures for invoking it, particularly with respect to oral communications, are somewhat clear.

<sup>24/</sup> Although we mention questions of overbreadth and vagueness raised by the technical data provisions of the ITAR previously in this memorandum, we have not attempted to identify and analyze particular problems for several reasons. First, our opinion that a prior restraint on public cryptography might survive First Amendment scrutiny is a limited one and does not purport to apply to the many other types of technical data covered by the ITAR. Second, we believe that public cryptography presents special considerations warranting separate treatment from other forms of technical data, and that a precise and narrow regulation or statute limited to cryptography would be more likely to receive considered judicial attention. Finally, we are uncertain whether the present legislative authority for the technical data provisions of the ITAR is adequate.